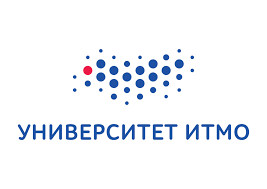
**Министерство науки и высшего образования Российской Федерации**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
**НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО**



**Факультет безопасности информационных технологий**

**Дисциплина:**

«Теория информационной безопасности и методология защиты

информации»

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №6**

«Разграничение доступа. Идентификация и аутентификация»

**Выполнили:**

Нгуен Тхи Маи, студент группы: N3245

*\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

**Проверил:**

Есипов Дмитрий Андреевич, ассистент ФБИТ

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(отметка о выполнении)

*\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

**СОДЕРЖАНИЕ**

[**Введение 4**](#_heading=h.gjdgxs)

[**Ход работы 5**](#_heading=h.ni3fiiymeat5)

[1. Основные Понятия 5](#_heading=h.tszytvy4o2l7)

[2. Идентификация/Аутентификация С Использованием Биометрии 6](#_heading=h.op0hxowc32xa)

[3. Схему Компьютерной Системы Со Встроенной В Нее Подсистемой Идентификации И Аутентификации. 7](#_heading=h.4nc0jy9jgssp)

[**Вывод 9**](#_heading=h.6ezmdqwmn5bj)

[**Список использованных источников 10**](#_heading=h.n1751prodfc8)

# Введение

*Цель:* разработка подсистемы идентификации и аутентификации субъектов.

*Задачи:*

1. Составить алгоритм для реализации выбранной подсистемы.

2. Составить полную схему компьютерной системы со встроенной в нее

подсистемой идентификации и аутентификации.

# Ход работы

## ОСНОВНЫЕ ПОНЯТИЯ

* **Идентификация –** это присвоение пользователю некоторого уникального идентификатора, который он должен предъявить СЗИ (средства защиты информации) при осуществлении доступа к объекту, то есть назвать себя. Используя предъявленный пользователем идентификатор, СЗИ может проверить наличие данного пользователя в списке зарегистрированных и авторизовать его (то есть наделить полномочиями) для выполнения определенных задач.
* **Аутентификация –** это подтверждение пользователем предъявленного идентификатора, проверка его подлинности и принадлежности именно данному пользователю. Аутентификация выполняется для устранения фальсификации на этапе идентификации.
* **Подсистемой идентификации и аутентификации (И/АУ)** – единая подсистема, объединяющая идентификацию и аутентификацию пользователя.

Стойкость к взлому подсистемы идентификации и аутентификации определяется гарантией того, что злоумышленник не сможет пройти аутентификацию, присвоив чужой идентификатор, либо украв его.

* **Основные методы** идентификации и аутентификации пользователя являются:
* Парольные системы;
* Идентификация/аутентификация с использованием технических устройств (идентификаторы iButton (Touch Memory), бесконтактные радиочастотные карты proximity, пластиковые карты, ключи e-Token);
* Идентификация/аутентификация с использованием индивидуальных биометрических характеристик пользователя (отпечатки пальцев, геометрическая форма рук, узор радужной оболочки и сетчатки глаз, форма и размеры лица, особенности голоса,  биомеханические характеристики почерка, биомеханические характеристики «клавиатурного почерка»).

## ИДЕНТИФИКАЦИЯ/АУТЕНТИФИКАЦИЯ С ИСПОЛЬЗОВАНИЕМ БИОМЕТРИИ

* **Биометрия** – это использование для аутентификации личности индивидуальных признаков человека. В качестве биометрических

характеристик, которые могут быть использованы при аутентификации

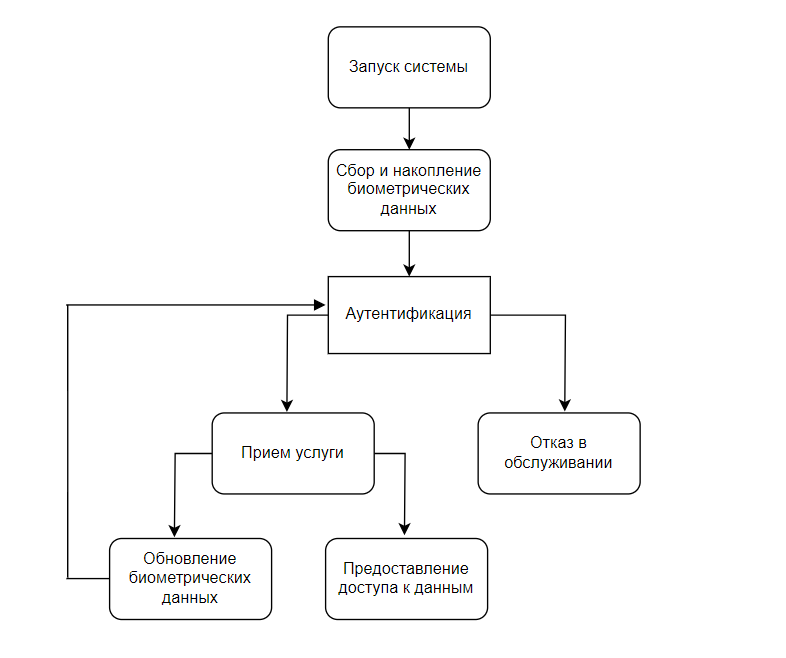
субъекта доступа, достаточно часто применяют следующие:

* **Особенности** применения биометрических систем идентификации и

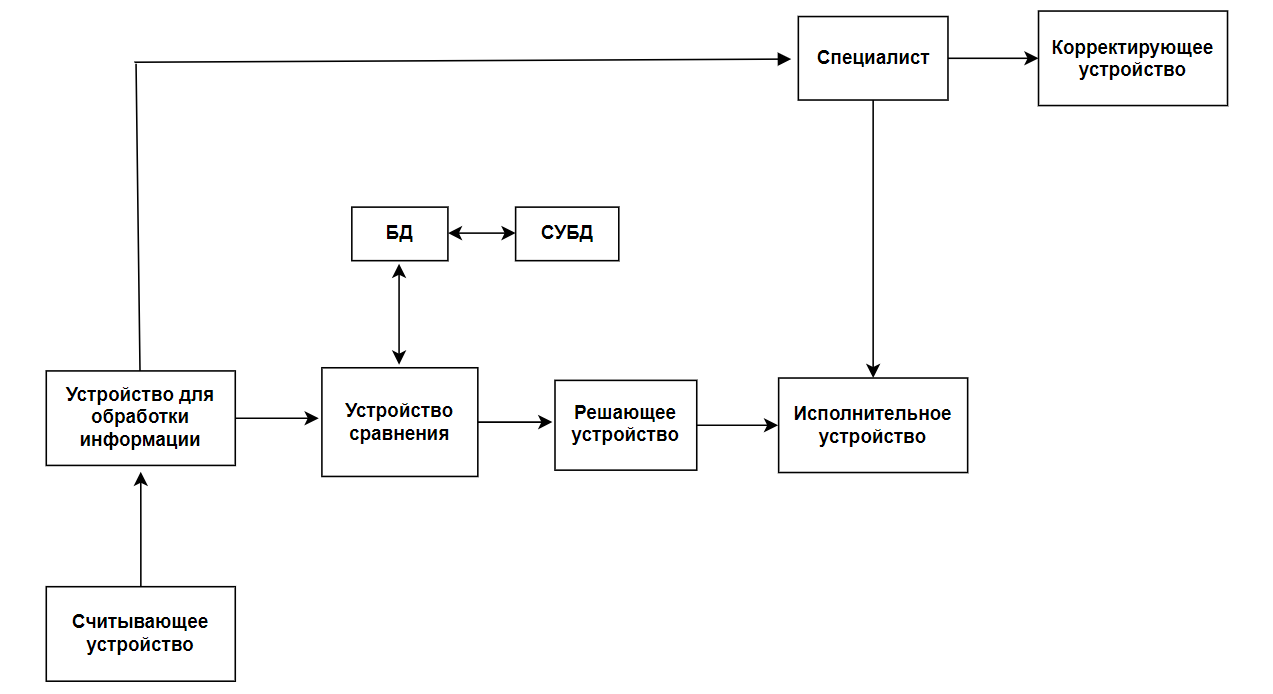
аутентификации личности:отпечатки пальцев;

* геометрическая форма рук;
* узор радужной оболочки и сетчатки глаз;
* форма и размеры лица;
* особенности голоса;
* биомеханические характеристики почерка;
* биомеханические характеристики «клавиатурного почерка».
* Необходимость обучения биометрической системы для
* конкретных пользователей, зачастую, достаточно длительного.
* Возможность ошибочных отказов и ошибочных подтверждений
* при аутентификации пользователей.
* Необходимость использования специальных технических
* устройств для чтения биометрических характеристик, как правило,
* достаточно дорогостоящих (за исключением, быть может, аутентификации
* по клавиатурному почерку).
* **Два основных типа биометрических систем**:
* Статические
* Динамические
* **Статические:**
* Отпечатки пальцев или рисунок папиллярных линий
* Радужная оболочка глаза
* Сетчатка глаза
* Рисунок вен
* Лицо
* Геометрия руки
* Сердечный ритм
* ДНК
* Мультимодальная идентификация
* **Динамические**:
* Почерк и динамика подписи
* Сердечный ритм
* Голос и ритм речи
* Распознавание жестов
* Скорость и особенности работы на клавиатуре компьютера
* Походка

## СХЕМУ КОМПЬЮТЕРНОЙ СИСТЕМЫ СО ВСТРОЕННОЙ В НЕЕ ПОДСИСТЕМОЙ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ.



*Рис.1 Алгоритм биометрической системы аутентификации пользователя*

**

*Рис.2 Схема биометрической системы аутентификации пользователя*

# Вывод

Биометрическая аутентификация очень перспективна и обладает рядом преимуществ перед другими методами. Например: надежность и высокая скорость аутентификации, легкость использования для пользователя, данные биометрических характеристик невозможно забыть или потерять. Однако у данной системы есть и свои недостатки: крупные затраты на оборудование и долгое обучение, невозможность изменения в текущей базе данных биометрических характеристик системы.

# Список использованных источников

1. <http://www.spiiras.nw.ru/dissovet/wp-content/uploads/2015/10/dissertacija_shchemelinin-finalnaja-versija1.pdf>
2. <https://drive.google.com/file/d/1Inhho7b5ik_aE98vmEpoaMc6KWEGvnMz/view>
3. <https://worldvision.com.ua/ru/preimushchestva-i-nedostatki-biometricheskoy-sistemy-autentifikatsii/>